Appl. No. : **09/577,449**
Filed : **May 24, 2000**

REMARKS

Reconsideration and allowance of the above referenced application are respectfully requested. After entry of this amendment, Claims 1-8, 10, 11, and 13-25 will pending.

Claims 1-22 stand rejected under 35 U. S.C. 102 as allegedly being anticipated by Bjorn. Initially, while this portion refers to claims 1-22 as being rejected, it is believed that the rejection intended to refer to all of claims 1-25, and this rejection has been answered as though that were the case. Therefore, this contention is respectfully traversed, and it is respectfully suggested that the rejection does not meet the Patent Office's burden of providing a prima facie showing of unpatentability.

Specifically, claim 1 requires obtaining information about a biometric part which is admittedly found in Bjorn as well as in the present claims. However, claim 1 also requires "forming a cryptographic key based on said biometric information without determining absolute dimensions of said biometric information". This latter portion is certainly not found in Bjorn, and in fact Bjorn teaches away from this feature.

Bjorn teaches a system that obtains a fingerprint, and extracts features from the fingerprint. These features include minuatae location, but also include location and orientation of minutae. In addition, the features may include spatial frequency, curvature (an absolute dimension), ridge count, distance (an absolute dimension), curvature between points (an absolute dimension), and the like, see for example column 3 lines 26-35. Based on these extracted features, a hashing technique creates a hash of the message. That hash is then used to define the encryption key. However,

notice that the hash is based on measurement which INCLUDE ABSOLUTE DIMENSIONS.

Therefore, it should be apparent from the above quoted portion that Bjorn intends not only to find but also to use those absolute dimensions. As part of the information obtained from the fingerprint, Bjorn describes determining the location of the minutae, their frequency, their curvature, distance between ridges, and the like. Many of these are in fact absolute dimensions of the biometric, and they represent the absolute dimensions of the biometric information. Nowhere is there any teaching or suggestion in Bjorn of determining the key without obtaining these absolute dimensions.

In fact Bjorn would not be able to create the hash that they intend on creating, without determining these absolute dimensions. Therefore, claim 1 is not taught or suggested by Bjorn. Bjorn expressly teaches determining absolute dimensions of the biometric information, and therefore claim 1 should be allowable thereover.

The rejection refers attention to column 4 lines 25-30, however this cited portion merely describes how the hash is turned into a cryptographic key. The hash itself is formed based on the fingerprint that is obtained from those dimensions including absolute dimensions, and therefore this does not teach or suggest the claimed features as noted above.

Claim 2 specifies that the forming comprises determining ratios between portions of the biometric information. The rejection points to column 4 beginning line 13, alleging that ratios between these different portions are found. However, this is respectfully traversed. Column 4 beginning line 14 describes the features which can be found, including many different features. Curvature between points and distance

between points are described. Relation to global features are described. Vector quantization is also described.

However there is no teaching or suggestion of ratios between different portions. In fact, nowhere is there any teaching or suggestion, anywhere in the prior art, of determining ratios between different portions of biometric information in this way.

Much of this is based on the inventor's recognition that existing fingerprint systems simply do not work reliably. In order to find a fingerprint and match against a reference, a great degree of precision is necessary. Fingerprint systems have not gained commercial success: mainly because of the large number of false positives and false negatives. Part of this is simply because it is not easy to determine absolute dimensions.

In contrast, claim 1 defines sensing without attempting to determine absolute dimensions. Instead, the present system determines relationships between the different features without determining the absolute dimensions. By doing this, it is believed that reliability could be improved. In any case, this is nowhere taught or suggested by the cited prior art.

Claim 3 specifies entering a plurality of different features in a sequence and that an order of the sequence forms the code. The rejection alleges that this is taught by column 4 lines 21-24 of Bjorn. However, all the cited portion states is that a template is created based on "at least some of the features extracted from the fingerprint". Nowhere is there any teaching or suggestion of entering any plurality of different biometric features in any sequence, much less that the order of the sequence forms the code. Therefore, each of these claims should be allowable for these reasons.

Claim 7 has been amended to include the limitations of claim 9 and, and claim 9 has correspondingly been canceled. The ratio between different parts of the biometric information was discussed above with respect to claim 2, and as discussed above, this is in no way taught or suggested by the cited prior art. Therefore, claim 7 as amended and should be allowable over the cited prior art .

Claim 11 has been amended to include the limitations of claim 12 thereon. The sequence of biometric parts was discussed above with respect to claim 3. As described herein, there is no teaching or suggestion of this in the cited prior art. Therefore, amended claim 11 should be allowable for these reasons.

Claim 14 defines an image sensor chip that forms a plurality of pixels for sensing an image. That chip has an active surface that, instead of sensing an image, as is the intention of such a chip, rather receives a finger thereon. Instead of getting an image from a distance, as the chip was intended to do, the chip is used to obtain a fingerprint directly. This is a quite unconventional use of an image sensor chip, and one which is not in anyway taught or suggested by the cited prior art.

The rejection alleges that Bjorn uses an image sensor chip to receive the fingerprint. However, it is respectfully suggested that this is incorrect. In fact, a fingerprint sensor 195 is used in this system see for example column 3 lines 6-11. Nowhere is there any teaching or suggestion of using an image sensor chip, which is made for sensing an image, to instead sense the fingerprint as claimed.

Claim 14 is based on the inventor's recognition that an image sensor chip which usually senses a large image from a small chip, based on the phenomenon of convergence of light rays, allows this small chip to image a very large image. However,

the user can put their finger directly on this chip surface, and the very high resolution of this chip enables determining a fingerprint image. There is no teaching or suggestion anywhere in the art of doing this. Moreover, image sensor chips can be quite inexpensive, since they are conventionally used in cameras, telephones, and the like.

Therefore, claim 14 should be allowable along with the claims which depend therefrom.

Claims 17-21 define using both the biometric, and the sequence of entry of the biometric, to form the key. This should hence be allowable for reasons set forth above.

Claims 22-25 determine not only the biometric parts but also additional information. The cryptographic key is based on both the biometric part and the additional information. The rejection states that this is obvious based on Bjorn. However, Bjorn teaches nothing about obtaining additional information and using that additional information along with the biometric information to form the cryptographic key. In attacking claims like 19 which include comparable limitations, the rejection draws attention to column 4 lines 27-35 of Bjorn. All this talks about, again, is the hash function; it talks nothing about entering additional information, and using that additional information to form the biometric key along with the main biometric input.

Some informalities noted in the claims, including lack of antecedent basis are also corrected herewith.

It is believed that all of the pending claims have been addressed in this paper. However, failure to address a specific rejection, issue or comment, does not signify agreement with or concession of that rejection, issue or comment. In addition, because the arguments made above are not intended to be exhaustive, there may be reasons

Appl. No. : 09/577,449
Filed : May 24, 2000

for patentability of any or all pending claims (or other claims) that have not been expressed. Finally, nothing in this paper should be construed as an intent to concede any issue with regard to any claim, except as specifically stated in this paper, and the amendment of any claim does not necessarily signify concession of unpatentability of the claim prior to its amendment.

In view of the above amendments and remarks, therefore, all of the claims should be in condition for allows. A formal notice to that effect is respectfully solicited.

No fees are believed necessary. However, please charge any fees due in connection with this response to Deposit Account No. 50-1387.

Respectfully submitted,

Date: 3-4-04

Scott C. Harris
Reg. No. 32,030

Customer No. 23844
Scott C. Harris, Esq.
P.O. Box 927649
San Diego, CA 92192
Telephone: (619) 823-7778
Facsimile: (858) 678-5082